ABSTRACT OF THE INVENTION

A system and method for securely roaming private data from a first client computer to a second client computer linked via a communication network. A user of the first client computer executes a home client application and designates private data for roaming. The home client application generates a first key in response to a password, and encrypts the designated private data as a function of the first key. The server receives and stores the encrypted private data. A user of the second computer executes a roaming client application and requests transfer of the encrypted private data from the server. The roaming client application generates the first key in response to the password, and decrypts encrypted private data transferred from the server to obtain the private data. The invention further provides users the ability to retrieve encrypted private from the server even when the user cannot remember the password associated with the first key. Also, the server has no knowledge of the private data nor the keys.